
black hat
BRIEFINGS & TRAINING
Blue Screen of the Death is Dead
MODERATED BY
JEFF MOSS,
BLACK HAT FOUNDER AND DIRECTOR
MATT. SUICHE
HTTP://WWW.MSUICHE.NET

WHO AM I?

- SECURITY RESEARCHER
  - NETHERLANDS
- MICROSOFT MVP 2009
  - *ENTERPRISE SECURITY*
- MS09-050
  - SMBV2 COMMAND VALUE VULNERABILITY
    - (CVE-2009-2532)
- *RANDOM THINGS:*
  - *SANDMAN LIBRARY*
    - *Library to manipulate Windows Hibernation File*
  - *PANGOWINGS PROJECT*
    - *Aims at creating a toolkit to manipulate every files related to Windows Physical Memory for defensive purposes only.*
    - *This includes windd (win32dd/win64dd)* ***We are discussing of this.***

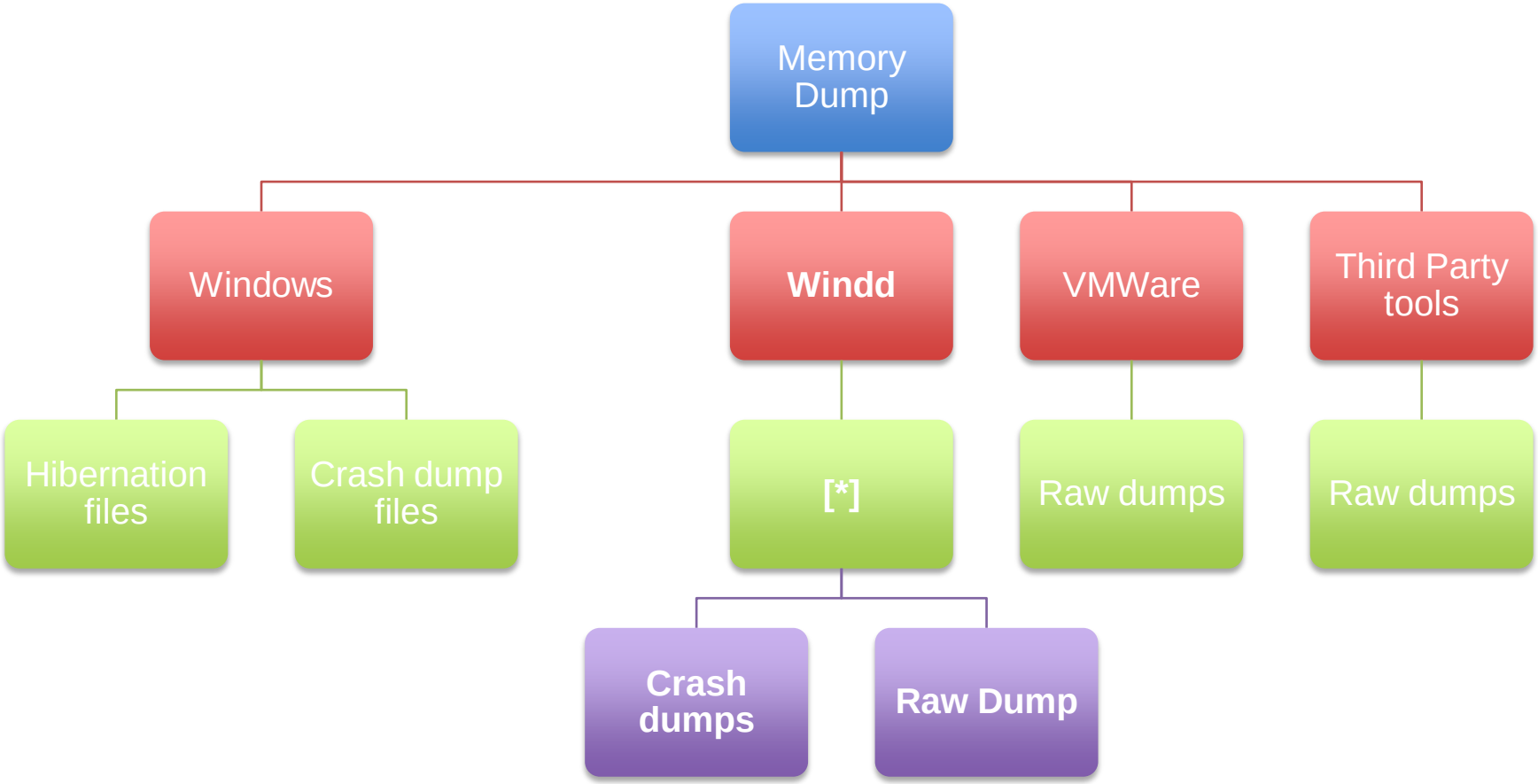
AGENDA

- What about Physical Memory?
- What about Memory Dumps?
- WinDD (Win32dd/win64dd) Utilities
- Windows Debugging Tools
  - Symbols
  - PowerDbg (PowerShell-based Interface for WinDbg)
  - WinDbg SDK
  - Huge Community
- Q&A

Physical Memory ?

- RAM
- Volatile memory so …
  - Registry
  - Processes information/list/map
  - Drivers information/list/map
  - Passwords
  - Mapped files
  - Everything you want but free beers.
- See M. Russinovich Blogpost
  - *Pushing the Limits of Windows: Physical Memory (Technet)*

Memory Dumps?



Memory Dumps?

- Windows hibernation file
  - Generated By Windows on Request
    - Compressed
      - LZNT1 (Windows 2000)
      - LZXpress/Xpress (Win XP, 2003, Vista, 2008, 7, 2008 R2)
      - TLZ (Upcoming windows 8 and 9)
    - Specific file format documented with SandMan
- Windows Crash Dump
  - Generated By B.S.O.D.
  - Mainly used and well-know for advanced troubleshooting.
    - Uses a file format (contains IMPORTANT information to set up Memory Manager, and debug-related variables, O.S. version, …)
    - Uncompressed
- Raw Dump
  - Only used in the Real World by Forensic Investigators
    - No File Format

Microsoft BSOD

black hat
BRIEFINGS & TRAINING

- Generates a Microsoft Crash Dump with BSOD but has some important limitations:
  - Reboot
  - No Full Memory Dump > 2GB of RAM.
  - Callback functions are not cool, Rootkit.C used them to prevent from "Memory leak"
    - See Frank Boldewin talk at hack.lu 2008

Windd Utility

- ONLY FOR RAM DUMPING.
- TWO TYPES OF OUTPUT FILES
  - RAW FILES
  - MICROSOFT CRASH DUMP FILES
    - No Blue Screen Of the Death
    - No Reboot
    - Even if the Machine is not running in Debug Mode
- NETWORK SUPPORT (SERVER AND CLIENT)
  - DATA ARE SENT FROM KERNEL-MODE
  - DATA CAN BE RECEIVED BY WINDD ITSELF FROM USER-MODE.
- SAMBA PATH SUPPORT

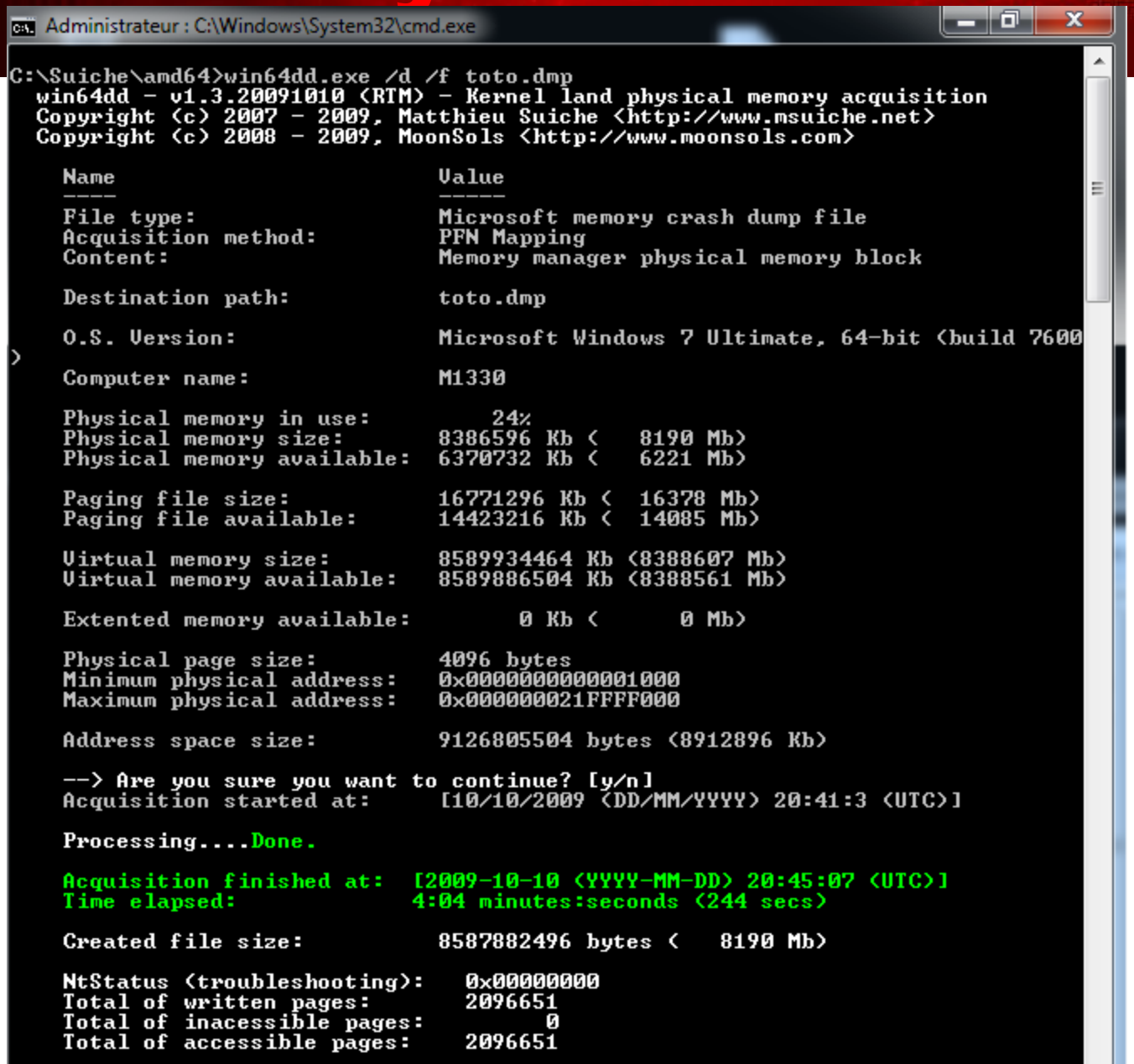
Windd Utility

- Fast
- Support for Machine with more than 4GB of RAM
- Hash Computing Support
  - MD5, SHA-1, SHA-256
- Different Mapping Methods
- Can choose the content of the dump
  - Only the PFN database
  - Or extend the content
- And Free!

Windd Utility

- Misc. Features like
  - Generate a BSOD
  - Hibernate the Machine with no Password prompt when resumed
- Compatible with
  - Win2000 (x86), WinXP, Win2003, WinVista, Win2008, Win7, Win 2008 R2 (Both x86 and x64 architecture)
- And Windd is **FREE**

Windd Utility



WinDbg Tools

- Windows Debugger (WinDbg)
- Microsoft Symbols (*.pdb files)
  - Automatically downloadable from Microsoft Servers
- Also provides a SDK to develop plug-ins for WinDbg or standalone application.
- Maintained by Microsoft
  - I feel lazy to reinvent the wheel with a graphical interface and a scripting language.

WinDbg Tools

- Microsoft Symbols
  - Structures definition
  - Un-exported names
  - Function Types etc..
- What you Do Not Want to Rewrote
  - DbgHelp.dll (Windows Image Helper)
  - DbgEng.dll (Win Symbolic Debugger Engine)
  - SymSrv.dll (Symbols Server)
  - All extensions and add-ons.
- *IDA uses the stuff above.*

Registry Access


```
kd> !reg

reg <command> <params>        - Registry extensions
    kcb        <Address>      - Dump registry key-control-blocks
    knode      <Address>      - Dump registry key-node struct
    kbody      <Address>      - Dump registry key-body struct
    kvalue     <Address>      - Dump registry key-value struct
    valuelist  <HiveAddr> <KnodeAddr> - Dumps list of values for a particular
    knode
    subkeylist <HiveAddr> <KnodeAddr> - Dumps list of subkeys for a particular
    knode
    baseblock  <HiveAddr>     - Dump the baseblock for the specified hive
    seccache   <HiveAddr>     - Dump the security cache for the specified hive
    hashindex  <conv_key>     - Find the hash entry given a Kcb ConvKey
    openkeys   <HiveAddr|0>   - Dump the keys opened inside the specified hive
    openhandles <HiveAddr|0>  - Dump the handles opened inside the specified hive
    findkcb    <FullKeyPath>  - Find the kcb for the corresponding path
    hivelist                  - Displays the list of the hives in the system
    viewlist   <HiveAddr>     - Dump the pinned/mapped view list for the specified
    hive
    freebins   <HiveAddr>     - Dump the free bins for the specified hive
    freecells  <BinAddr>      - Dump the free cells in the specified bin
    dirtyvector<HiveAddr>     - Dump the dirty vector for the specified hive
    cellindex  <HiveAddr> <cellindex> - Finds the VA for a specified cell index
    freehints  <HiveAddr> <Storage> <Display> - Dumps freehint info
    translist  <RmAddr|0>     - Displays the list of active transactions in this RM
'''
```

Process Information

- !process
- !thread
- Integrated Disassembler
- !peb
- Windbg.hlp

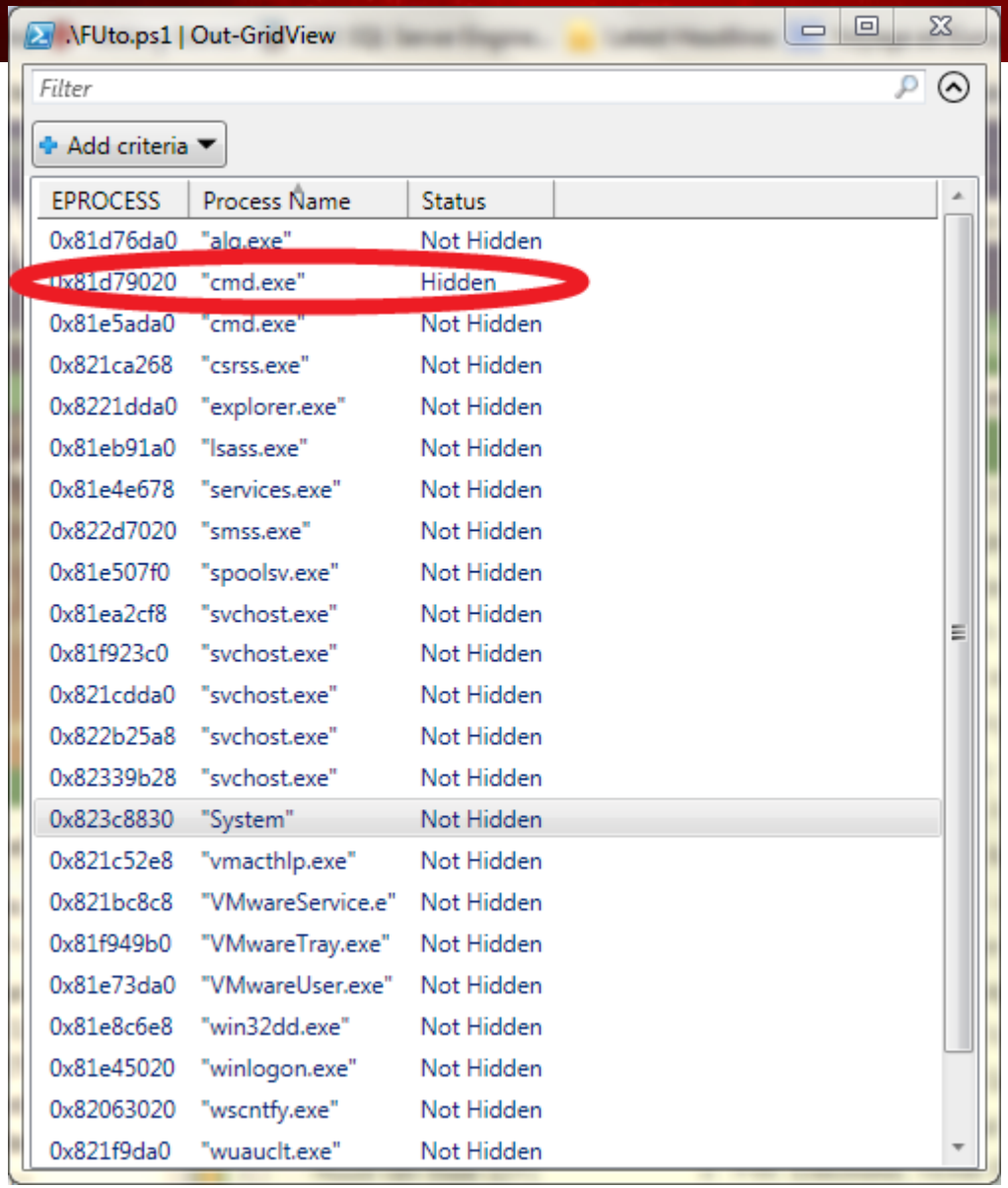
Windbg Tools


```
Windows 7 Kernel Version 7600 MP (2 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 7600.16385.amd64fre.win7_rtm.090713-1255
Machine Name:
Kernel base = 0xfffff800`02a5a000 PsLoadedModuleList = 0xfffff800`02c97e50
Debug session time: Sat Oct 10 16:54:03.323 2009 (GMT-4)
System Uptime: 0 days 21:14:38.113
Loading Kernel Symbols
..
0: kd> !process 0 0
**** NT ACTIVE PROCESS DUMP ****
PROCESS fffffa8006705040
    SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 00187000  ObjectTable: fffff8a0000018c0  HandleCount: 2145.
    Image: System

PROCESS fffffa8007c37310
    SessionId: none  Cid: 010c    Peb: 7fffffd5000  ParentCid: 0004
    DirBase: 1f7d19000  ObjectTable: fffff8a0004dde10  HandleCount:  30.
    Image: smss.exe

PROCESS fffffa80085fdb30
    SessionId: 0  Cid: 0164    Peb: 7fffffdf000  ParentCid: 0150
    DirBase: 1eba00000  ObjectTable: fffff8a00189db10  HandleCount: 678.
    Image: csrss.exe
```

DKOM Attacks?

- Symbols + SDK
  - Can write you own extension.
- See next slide
  - Microsoft Crash Dump vs Futo Rootkit
  - (Shakacon 2009, *Challenge of Windows Physical Memory Acquisition and Exploitation*)

DKOM?


.\FUto.ps1 | Out-GridView
Filter
Add criteria
EPROCESS
Process Name
Status
0x81d76da0 "alg.exe" Not Hidden
0x81d79020 "cmd.exe" Hidden
0x81e5ada0 "cmd.exe" Not Hidden
0x821ca268 "csrss.exe" Not Hidden
0x8221dda0 "explorer.exe" Not Hidden
0x81eb91a0 "lsass.exe" Not Hidden
0x81e4e678 "services.exe" Not Hidden
0x822d7020 "smss.exe" Not Hidden
0x81e507f0 "spoolsv.exe" Not Hidden
0x81ea2cf8 "svchost.exe" Not Hidden
0x81f923c0 "svchost.exe" Not Hidden
0x821cdda0 "svchost.exe" Not Hidden
0x822b25a8 "svchost.exe" Not Hidden
0x82339b28 "svchost.exe" Not Hidden
0x823c8830 "System" Not Hidden
0x821c52e8 "vmacthlp.exe" Not Hidden
0x821bc8c8 "VMwareService.e" Not Hidden
0x81f949b0 "VMwareTray.exe" Not Hidden
0x81e73da0 "VMwareUser.exe" Not Hidden
0x81e8c6e8 "win32dd.exe" Not Hidden
0x81e45020 "winlogon.exe" Not Hidden
0x82063020 "wscntfy.exe" Not Hidden
0x821f9da0 "wuauclt.exe" Not Hidden

Past/Present/Future?

black hat
BRIEFINGS & TRAINING

- More Defensive Extensions for WinDbg in 2010?
  - Roberto A. Farah wrote a PowerShell interface for WinDbg
  - Microsoft "!exploitable"
  - ...

Conclusion

black hat
BRIEFINGS & TRAINING

- Sometimes it is just really cool to look around to see what people have already done.
- Free libraries and scriptable Software maintained by Microsoft
  - So What?

Questions?

MATT/MSUICHE/NET

HTTP://WWW.MSUICHE.NET

HTTP://WINDD.MSUICHE.NET

Links

- WinDD
  - http://pangowings.msuiche.net
- PowerDbg
  - http://www.codeplex.com/powerdbg
- Windows Debugging Tools
  - http://www.microsoft.com/whdc/devtools/debugging/default.mspx
- Shakacon, Challenge of Windows Physical Memory Acquisition and Exploitation
  - http://msuiche.net/con/shakacon2009/NFI-Shakacon-win32dd0.3.pdf
- srv*c:\symbols*http://msdl.microsoft.com/download/symbols